IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

HARRY C. NAGEL, Plaintiff, v. SIEMENS INDUSTRY, INC., SIEMENS RAIL AUTOMATION CARBORNE SYSTEMS, INC., AND SIEMENS RAIL AUTOMATION CORPORATION Defendants.	)	Civil Action No. 2:15-cv-01669- RCM *Electronically Filed*

DEFENDANTS' BRIEF IN SUPPORT OF EMERGENCY MOTION TO COMPEL THE EXPEDITED RETURN OF DEFENDANTS' PROPERTY, PRESERVATION OF ELECTRONIC DATA SOURCES, PRODUCTION OF DATA SOURCES TO A FORENSIC EXAMINER, AND FOR SANCTIONS

Defendant Siemens Industry, Inc. (for itself and as successor by merger to improperly named Defendants Siemens Rail Automation Carborne Systems, Inc., and Siemens Rail Automation Corporation, which no longer exist as separate legal entities) ("Siemens") submits this Brief in Support of Emergency Motion to Compel the Expedited Return of Defendants' Property, Preservation of Electronic Data Sources, Production of Data Sources to a Forensic Examiner, and for Sanctions. Siemens incorporates by reference the concurrently-filed Statement of Material Facts in its entirety. Given the nature of Plaintiff's misconduct and ongoing wrongful possession of more than 30,000 misappropriated, proprietary documents, Siemens respectfully requests an expedited ruling.

I. BACKGROUND

Plaintiff was a General Manager with Siemens from approximately May 2, 2013 until April 3, 2015. *See* Defendants' Statement of Material Facts ("SOF") ¶1. Plaintiff resigned from

Siemens on April 3, 2015, [redacted]" *Id.* at ¶¶ 1, 7-8.

Seven months after his resignation Plaintiff served Siemens with a Complaint. The Complaint asserts claims for alleged breach of his Employment Agreement and violation of the Pennsylvania Wage Payment and Collection Law. *Id.* at ¶ 4. Through discovery, Siemens has learned that on his last day of his employment, Plaintiff downloaded to three personal flash drives more than 30,000 emails and other documents belonging to Siemens.[1] *Id.* at ¶¶ 17, 21-23. Plaintiff took these documents without permission and [redacted] obligations to Siemens, as well as numerous company policies. *Id.* For reasons unclear, Plaintiff also transferred copies of these documents to his personal MacBook computer. *Id.* at ¶ 36. Siemens has also learned that Plaintiff's counsel disclosed these documents to third parties, may have altered important data on the flash drives, and released the MacBook computer back to Plaintiff for his continued use. *Id.* at ¶¶ 31-47.

After learning the extent of Plaintiff's misappropriations and confirming that confidential information was taken, Siemens' counsel promptly requested the return of its property. *Id.* at ¶¶ 26, 29. Siemens' counsel also attempted to reach a mutually agreeable solution for recovering the wrongfully obtained documents and preserving the flash drives and MacBook computer. *Id.* at ¶ 33. Plaintiff's counsel rejected Siemens' proposal and has refused to return or sequester Siemens' documents or the data sources to which they have been copied by Plaintiff. *Id.* at ¶47.

---

[1] *See* The Sedona Conference® Glossary (4th Ed.) (defining a "flash drive" as "[a] small removable data storage device that uses flash memory and connects via a USB port. Can be imaged and may contain residual data.").

29.

The flash drives and MacBook computer may contain critical information, such as metadata, that proves Siemens defenses and potential counterclaims arising out of Plaintiff's misappropriation of Siemens' protected documents.[2] Some of this evidence may have already been destroyed by Plaintiff or his counsel, and some may soon be destroyed by Plaintiff through his continued use of his MacBook computer. Thus, timely intervention by this Court is needed.

Although the parties have met and conferred at length, Plaintiff rejected Siemens' requests to return the misappropriated documents, stop disseminating confidential and proprietary information, and cease activities which may destroy electronic evidence. *Id.* at ¶47. Plaintiff's counsel also provided conflicting representations about Plaintiff's relevant data sources, its preservation of same, and its willingness to meet and confer to reach a resolution of these matters. Moreover, Plaintiff's counsel has started using Siemens' misappropriated documents as surprise exhibits at witness depositions in this case. *Id.* at ¶¶ 34, 48. Siemens therefore brings this Motion to compel the return of its property; for an order protecting against further dissemination of its property and destruction of relevant evidence, permitting forensic inspection of Plaintiff's data sources by a neutral third party forensic examiner, and allowing eventual remediation of Siemens' documents from Plaintiff's data sources; and to award sanctions.

II. ARGUMENT

A. Blackletter "Conversion" Law Requires Plaintiff To Return Misappropriated Property

E-discovery considerations aside, blackletter law and equity also require the return of Siemens' documents. Put simply, Plaintiff took Siemens' property without authorization. The

[2] Siemens' Motion for Leave to File Amended Answer to Plaintiff's Complaint and Affirmative and Additional Defenses is currently pending before this Court. [Dkt. No. 19].

law is clear: an employee cannot take an employer's property and refuse to return it. *See Bell v. Lockheed Martin Corp.*, No. 08-6292 (RBK/AMD), 2010 WL 11450407 (D.N.J. June 30, 2010).

Indeed, Courts recognize no difference between misappropriation of electronic property and misappropriation of physical property. As one district court explained, an employee-plaintiff cannot keep employer documents for his personal benefit, including anticipated litigation:

> [A]uthorization and access does not extend to allowing Plaintiffs [employees] to take company property for their personal benefit. Had Plaintiffs removed from their offices tangible assets, such as the desks at which they worked, or the computer monitors on their desks, there would be no dispute that they wrongly took Defendant's property, even though permitted to use such property in the course of their employment, and even though such property is not confidential or proprietary. . . . The fact that the property at issue was in an electronic format, or was converted from an electronic format to paper, does not alter the analysis that Defendant's property was taken by Plaintiffs without authorization from Defendant. To find otherwise would in essence advance the theory that "anything not nailed down can permissibly be stolen."

Bell, 2010 WL 11450407 at *5 (*quoting Herrera v. Clipper Group,* No. Civ. A. 97-560, 97-561, 1998 WL 229499, at *2 (S.D.N.Y. May 6, 1998)). *See also, Prudential Ins. Co. of Am. v. Stella*, 994 F. Supp. 318, 323–24 (E.D. Pa. 1998) ("Conversion" under Pennsylvania law includes "transferring the chattel and thereby depriving the owner of control; unreasonably withholding possession of the chattel from one who has the right to it; and misusing or seriously damaging the chattel in defiance of the owner's rights.")

In *Bell*, a district court required plaintiff employees to return 2,500 electronic documents taken from the defendant employer's computer systems. As here, the employer only learned during the course of litigation that documents were taken. The court rejected plaintiffs' arguments about whether the documents were sensitive, confidential or proprietary, holding that "the more critical inquiry is whether the documents at issue were Defendant's property and whether Plaintiffs were authorized to take Defendant's property." *Bell*, 2010 WL 11450407 at

*5.[3] The court found that where the documents were taken "through the company computers using a company password[,]" the plaintiffs had to return all copies of "company documents." *Id.*

Here, since neither Plaintiff nor Plaintiff's counsel are authorized to possess the more than 30,000 Siemens documents at issue, the law plainly requires that they be returned. It is evident neither Plaintiff nor his counsel will do so absent an order from this Court. Siemens therefore seeks the Court's aid in getting all copies returned.

B. The Court Should Enter A Preservation and Forensic Inspection Order to Prevent Further Destruction of Critical Evidence and Further Dissemination of Siemens' Protected Documents

Siemens requests a preservation and forensic inspection order to prevent destruction of evidence in Plaintiff's possession and the disclosure of Siemens' proprietary information. Courts consider three factors when deciding whether to issue a preservation order:

1. the level of concern for the continuing existence and maintenance of the integrity of the evidence;

2. any irreparable harm likely to result to the party seeking the preservation of evidence; and

3. the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation.

Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433–34 (W.D. Pa. 2004). Production of electronic data for forensic inspection is typically ordered in cases "where data is likely to be destroyed or where computers have a special connection to the lawsuit." *Memry Corp. v. Kentucky Oil Tech., N.V.*, 2007 WL 832937 (N.D. Cal. March 19, 2007); *accord*

[3] Here, Plaintiff, in his role as General Manager of a Siemens' business unit, had access to Siemens' privileged, confidential and proprietary information. *See* SOF ¶ 24. Regardless, it is undisputed that the documents in question are Siemens' property.

Ingrid & Isabel, LLC v. Baby Be Mine, LLC, No. 13-CV-01806-JCS, 2014 WL 1338480, *9 (N.D. Cal. Apr. 1, 2014). Where misappropriated protected documents are involved and the "connection between the computers and the claims…[is not] unduly vague or unsubstantiated," courts will grant forensic inspections. *Weatherford U.S., L.P. v. Innis*, No. 4:09-cv-061, 2011 WL 2174045, *4 (D.N.D. June 2, 2011), *citing, Balboa Threadworks, Inc. v. Stucky*, No. 05–1157, 2006 WL 763668, at *3 (D.Kan. March 24, 2006) ("This is one method of assuring the preservation of evidence since electronic evidence [may] [sic] easily be erased and manipulated, either intentionally or unintentionally (by overwriting through continued use of the computer)").

Plaintiff and his counsel have compromised the integrity of Siemens' protected documents and the data sources to which Plaintiff wrongfully copied them. *See* SOF, ¶¶ 28-29. [4]As explained above, and in the Statement of Material Facts, Plaintiff copied the protected information (i.e. confidential, proprietary and/or privileged documents) from Siemens' computer systems to three flash drives right before leaving Siemens, and subsequently copied the files again to his MacBook computer. *See* SOF, ¶¶ 21-23, 36. With his counsel's knowledge and approval, Plaintiff continues to use this computer, despite Siemens' legitimate concern that using the computer may alter or destroy evidence critical to Siemens' defenses. *See* SOF, ¶47. Plaintiff's counsel itself may have compromised the integrity of the flash drives by connecting the flash drives to its law firm computers, thereby potentially altering evidence, including metadata, revealing what documents were taken from Siemens and when. *See* SOF ¶ 31, Exhibit 14 pp. 1-2. Plaintiff's counsel has demonstrated that it cannot be trusted to preserve Plaintiff's data sources.

---

[4] *See* Exhibit 14, August 8, 2016 Email from Littler, pp. 2-3. Confirming that Plaintiff's counsel took possession of the flash drives and connected them to their law firm's computer systems. The files were then uploaded to Nextpoint's (their firm's third party eDiscovery vendor) "cloud" hosted document review system.

Plaintiff's counsel has also disclosed Siemens protected information to two third parties. Specifically, the documents were provided to Plaintiff's eDiscovery vendors. *Id.* Despite being asked to return and destroy Plaintiff's counsel's copies and the vendors' copies of these documents, Plaintiff's counsel has refused to do so. *See* SOF, ¶¶ 32-33, 47. In fact, Plaintiff's counsel has used Siemens protected documents, without warning, as exhibits at witness depositions. *See* SOF, ¶¶ 34, 48. It is unclear whether Plaintiff's counsel will continue to disclose Siemens' protected documents to others or to copy Siemens' documents to other data sources. Plaintiff's counsel cannot be trusted to refrain from doing so without judicial intervention.

Plaintiff and his counsel have offered no legitimate basis for continuing to improperly withhold, disseminate, and use Siemens' protected documents, or to potentially destroy evidence demonstrating Plaintiff's misappropriation of more than 30,000 Siemens documents.

To date, the only rationale communicated to Siemens by Plaintiff for not temporarily surrendering his MacBook is that Plaintiff would prefer not to be inconvenienced by doing so. Plaintiff's temporary inconvenience is hardly a significant burden, and certainly not one that outweighs the confidentiality, privilege, and evidence destruction concerns at issue here. It is also important to note that this is a situation of Plaintiff's own creation: he misappropriated documents from his former employer and stored them on his personal computer. He could easily have avoided any purported inconvenience by never having wrongfully taken Siemens' proprietary information and/or stored such information on his personal computer.

Given the circumstances, a preservation and forensic order should be granted. The order should require Plaintiff to relinquish the following data sources to a neutral, certified forensic

examiner for preservation, segregation and return of non-Siemens documents[5] to Plaintiff, return of Siemens' documents to Siemens, and forensic analysis and eventually for remediation at the conclusion of this case:

- Plaintiff's flash drives;
- Plaintiff's old laptop computer (that is purportedly no longer in use by Plaintiff);
- Plaintiff's MacBook (to which he backed up his flash drives); and
- any other data source(s) to which Plaintiff may have transferred Siemens' property.

In addition, Plaintiff's counsel should be ordered to delete and destroy any Siemens' documents in its possession that Plaintiff took from Siemens.[6] Plaintiff should also be prohibited and estopped from using any such improperly-obtained documents in connection with this case. *See Bell v. Lockheed Martin Corp.*, No. 08-6292 (RBK/AMD), 2010 WL 11450407 (D.N.J. June 30, 2010) (ordering plaintiff employees to return all copies of company's electronic documents and explaining that the employees "must request them from through the discovery mechanisms set forth in the Federal Rules of Civil Procedure."). Finally, to the extent Plaintiff has copied any of the above-referenced data sources, or to the extent his counsel had his MacBook forensically

---

[5] Notably, electronic documents created by Plaintiff on Siemens' systems while he was employed by Siemens were "part of the official records of the Company[,] regardless of whether Plaintiff believes they are of a "business or personal nature[.]". *See* SOF, ¶ 23 Ex. 8, p. 2, (Siemens' Electronic Communications policy) (noting Siemens "reserves the right to monitor all Internet traffic, and retrieve and read any data composed, sent or received through our online connections and stored on our computer systems, including email…whether of a business or personal nature…All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of the Company…"). Thus, any documents taken from Siemens' computer systems would be Siemens' documents not "personal" documents exempt from the obligations requiring return of Siemens' documents to Siemens.

[6] To the extent Plaintiff reasonably believes, after a good faith investigation by his counsel, that he was expressly permitted to retain a given document from the time-period of his employment with PHW (which was from 1991 until May 2012), Plaintiff's counsel should confer with Siemens' counsel as to the permissible retention of that document.

imaged by other parties, those copies should also be secured to ensure that Plaintiff does not misuse or further disseminate Siemens' data.

C. Plaintiff's Data Sources Must Be Forensically Secured to Protect Against Further Alteration of Evidence, Including Metadata

"In general, metadata is relevant when the process by which a document was created is in issue or there are questions concerning a document's authenticity. Metadata may reveal when a document was created, how many times it was edited, when it was edited and the nature of the edits. In the absence of an issue concerning the authenticity of a document or the process by which it was created, most metadata has no evidentiary value." *Kingsway Fin. Services, Inc. v. PricewaterhouseCoopers LLP*, 2008 WL 5423316, 6 (S.D.N.Y. Dec. 31, 2008).

In cases involving employees misappropriating an employer's protected electronic documents, courts routinely order forensic preservation and inspection of the employee's data sources. In *Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, where a former employee had accessed, downloaded and transmitted his employer's proprietary information, the court ordered the employee to turn over his data sources for forensic imaging by a neutral expert. 267 F.R.D. 443 (D. Conn. 2010). The court explained that while there is no "routine right of direct access to a party's electronic information system…such access might be justified in certain circumstances" and that courts should consider the relationship between the claims (and logically: also *defenses*) at issue and the requested data sources. *Id.* at 446. As the Court noted, "forensic imaging by a neutral expert is the only way that [the employer] will be able to secure the electronic data to which it is entitled." *Id.* (Emphasis added.) *See also, e.g., Weatherford U.S., L.P. v. Innis*, 2011 WL 2174045, *4 (D.N.D. June 2, 2011) (employee's downloading of files without permission was "enough to provide a nexus between [the employer's] claims and its need for images of [the employee's] computers"); *Hudson Global Resources Hldgs., Inc. v. Hill*, 2007 WL 1545678

(W.D. Pa. May 25, 2007) (where former employee transferred 11,380 files from his work computer to an external hard drive on the day before he resigned, and despite lack of evidence of employee's consent to confidentiality policy, court ordered the return of documents taken from the employer's computer systems, ordered production of an affidavit by employee listing any other documents belonging to employer in his possession, "which must be returned to [employer] with no copies retained by [employee] or anyone on his behalf" and directed counsel to agree on forensic protocol to remediate employer's documents); *Penn-Air & Hydraulics Corp. v. Lutz*, 2015 WL 4508922 (M.D. Pa. July 24, 2015) (where former employee took company documents from his company computer and copied its contents before wiping certain data on the computer and returning it, court ordered employee to surrender all electronic devices that contain copies of any files belonging to employer, including several flash drives, and hard copies to employer and directed employee to refrain from further copying, use, or retention or failure to return of employer's documents); *Quaker Chemical Corp.v. Varga*, 509 F.Supp.2d 469 (E.D. Pa. 2007) (ordering former employee to return flash drive onto which he had transferred 4,496 files from his work computer, and which he had endeavored to delete).

Here, metadata may be essential to Siemens' defenses, as it may verify when Plaintiff took Siemens' documents, what documents were taken, where they may be stored, and other information demonstrating Plaintiff's violation of his various obligations to Siemens. However, as discussed in greater detail above and in Siemens' Statement of Facts, both Plaintiff and his counsel have likely altered and will likely continue to alter relevant electronic evidence, including but not limited to metadata, supporting Siemens' defenses during the time this evidence remains in their possession. As explained above and in the Statement of Facts, Plaintiff's counsel knowingly accessed Plaintiff's flash drives containing misappropriated

documents and returned the MacBook computer (which contains copies of Siemens' protected documents) for Plaintiff's continued use – thereby placing evidence, including metadata, supporting Siemens' defenses as risk of destruction. Such conduct demonstrates that an Order from this Court is needed to insure *status quo* preservation of Plaintiff's data sources. Plaintiff's counsel knew that Siemens documents were stored on Plaintiff's flash drives before reviewing any such documents, and Plaintiff's counsel knew that Siemens documents had been copied to the MacBook computer by the time it returned the computer to Plaintiff for his continued use. Plaintiff's counsel also received guidance from an eDiscovery forensic consultant throughout this case. Plaintiff's counsel should have known that copying documents from the flash drives and allowing continued use of the MacBook computer would invite overwriting and alteration of relevant evidence. *See Quotient, Inc. v. Toon*, No. 13-C-05-64087, 2005 WL 4006493, at *1–2 (Md. Cir. Ct. Dec. 23, 2005) (describing how computers constantly overwrite space on the hard drive and ordering forensic images where "there is a substantial probability that [electronic] files that are relevant to this case could be made less accessible to the parties merely by Defendant's normal course of computer use.")

Ordering forensic collection and examination of Plaintiff's data sources used to store, transmit, save, or hold Siemens' protected information will serve several purposes. It will prevent Plaintiff and his counsel from further allowing or actively enabling the dissemination of Siemens' protected information across more data sources and to additional third parties, and will prevent Plaintiff and his counsel from potentially destroying evidence. It will also enable the forensic examiner to identify Siemens' documents on these data sources so they can eventually be remediated and removed after this matter has concluded. With a Court Order in place, Siemens anticipates that the parties can agree on a reasonable and appropriate forensic protocol

to accomplish these tasks.

D. Plaintiff's And His Counsel's Conduct Calls For The Imposition of Sanctions

A district court may impose sanctions for abuses of the judicial process. *Republic of Philippines v. Westinghouse Elec. Corp.*, 43 F.3d 65, 73 (3d Cir. 1994) (citing *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43-44, (1991)). Inherent powers must be exercised with restraint and discretion." *Id.* at 74. "A primary aspect of [a district court's] discretion is the ability to fashion an *appropriate* sanction for conduct which abuses the judicial process." *Id.* (Emphasis in original). Here, the Court should impose sanctions against Plaintiff and his counsel based on their intentional refusal to return Siemens' property, attempts to circumvent the discovery process, and failure to preserve relevant evidence.

1. Plaintiff's and his counsel's failure to return Siemens' property and preserve relevant evidence.

In *Burt Hill, Inc. v. Hassan*, 2010 WL 419433 (W.D. Pa. Jan. 29, 2010) (M.J. Bissoon) defendants' counsel received documents belonging to plaintiff (including documents that on their face were protected by the attorney client privilege) from an "anonymous source." *Id.* at *1. Defendant's counsel reviewed and retained the materials. *Id.* at *7. In reviewing plaintiff's motion to prohibit defendants' use of alleged "anonymous source" documents and motion to disqualify defense counsel, the court held that:

> Pennsylvania courts have recognized that an attorney receiving confidential documents has ethical obligations that may surpass the limitations implicated by the attorney-client privilege and that apply regardless of whether the documents retain their privileged status…

Burt Hill, Inc. v. Hassan, 2010 WL 419433, (W.D. Pa. January 29, 2010) (M.J. Bissoon) (emphasis added). *See also*, *United States v. Kubini*, 304 F.R.D. 208, 224 (W.D. Pa. 2015) (J. Fischer). "It is these principles that underlie the oft-cited protocol directing counsel, upon discovering the confidential nature of documents, to cease review, notify the owner, and abide by

the owner's instructions regarding the document's disposition." *Id. See also Knitting Fever, Inc. v. Coats Holding Ltd.*, 2005 WL 3050299, *1, 4 (E.D.N.Y. Nov.14, 2005) (where plaintiffs obtained documents from "an undisclosed ... employee" of defendants, plaintiffs' counsel had "a clear ethical responsibility to notify [defense] counsel and either follow the latter's instructions with respect to the disposition of the documents or [to] refrain from using them pending ruling by the [c]ourt"). Moreover, "[e]ven in the absence of privilege, courts have extended the "unauthorized disclosure" rules to materials that are "proprietary" or "confidential." *See Knitting Fever*, 2005 WL 3050299, *3; *S.E.C. v. Brady*, 238 F.R.D. 429, 445 (N.D. Tex.2006) (requiring counsel to return "proprietary documents obtained unfairly and outside the context of formal discovery").

As an initial matter, Plaintiff's counsel should have known and disclosed long before July 2016 that Plaintiff's flash drives contained over 30,000 Siemens documents, that he copied these documents to a personal MacBook, and that he was also in possession of an old laptop that he used for work purposes. *See* LCvR 26.2.A.1 cmt. 1 (duty to discuss ESI with client); LCv26.2 (duty to investigate client's data sources). Plaintiff's counsel also should have been well aware that Plaintiff took Siemens documents without authorization, due to Plaintiff's legal, policy and [redacted] obligations. *See* SOF, ¶¶ 7-8. However, even assuming Plaintiff's counsel was unaware of these data sources and of Plaintiff's lack of authorization, Siemens put Plaintiff's counsel on notice of both no later than August 1, 2016. *See* SOF ¶¶ 28. At that time, if not months before, Plaintiff's counsel had an ethical obligation to "abide by [Siemens'] instructions regarding the document's disposition." *Burt Hill, Inc. v. Hassan,* 2010 WL 419433, 4*(W.D. Pa. January 29, 2010) (M.J. Bissoon) (emphasis added).

Despite these ethical obligations, Plaintiff's counsel has knowingly and intentionally

withheld Siemens' property, refused to comply with Siemens' instructions regarding disposition of the evidence, rejected Siemens' s reasonable proposal to have a neutral third party eDiscovery forensic examiner preserve the data sources, and failed to adequately preserve evidence relevant to Defendants' defenses and potential counterclaims. Plaintiff's counsel also misled Siemens into believing that Plaintiff's counsel would agree to return Siemens' documents, secure Plaintiff's data sources, and work through a forensic protocol. *See* SOF, ¶ 44. Plaintiff's counsel also assured Siemens that it had not reviewed the Siemens' documents taken by Plaintiff, and yet a few days later, Plaintiff's counsel used such a document as a surprise exhibit at a witness deposition. *See* SOF, ¶¶ 31, 34.

2. Plaintiff's and his counsel's circumvention of the discovery process

"[T]he proper avenue for a former employee to obtain privileged and/or confidential documents in support of his or her claims is through the discovery process as set forth in the Federal Rules of Civil Procedure, not by self-help." *Nesselrotte v. Allegheny Energy, Inc.*, Civ. No. 06-01390, 2008 WL 2858401, at *8 (W.D. Pa. July 22, 2008) (J. Fischer). "There is simply no excuse for engaging in self-help and flouting the Federal Rules of Civil Procedure to obtain discovery." *Coleman-Hill v. Governor Mifflin Sch. Dist.*, 271 F.R.D. 549, 554 (E.D. Pa. 2010). Therefore, a court can "sanction a party that seeks to introduce improperly obtained evidence; otherwise the court, by allowing the wrongdoer to utilize the information in litigation before it, becomes complicit in the misconduct." *Fayemi v. Hambrecht & Quist, Inc.*, 174 F.R.D. 319, 324 (S.D.N.Y. 1997) (emphasis added) (precluding the plaintiff from using in litigation the information wrongfully obtained).

3. Plaintiff's shifting disclosures during discovery

Plaintiff's counsel facilitated and exacerbated Plaintiff's unlawful activity by

intentionally withholding more than 30,000 documents from Siemens and knowingly disseminating them to two third parties *See* SOF ¶¶ 31-32; Exhibit 14, August 8, 2016 Letter from Littler, pp. 1-2. Counsel's ever-changing positions have only compounded the problem during discovery. With respect to Plaintiff's documents and ESI:

- Plaintiff's counsel represented in February 2016 that "[c]opies of all documents that [Plaintiff] has in his possession, custody, or control which may be used to support his claims or defenses are... included on the CD which is being provided herewith." *See* SOF ¶ 10.
- In March 2016, Plaintiff's counsel represented that Plaintiff actually had one (1) personal computer, two (2) personal email accounts that he used for personal purposes, and three (3) flash drives containing unidentified "information" from PHW's, Invensys', and Siemens' computer systems dating back to 1991. *See* SOF ¶¶ 16-17.
- In July 2016, Plaintiff's counsel finally disclosed that one of Plaintiff's flash drives actually contained "over 30,000 emails, as well as documents from the Microsoft Office suite (.doc, .xls, .ppt, etc.)," and PDF documents. *See* SOF ¶ 21.
- In August 2016, Plaintiff's counsel informed Siemens' counsel, for the first time, that Plaintiff additionally had an "old, possibly nonfunctioning personal laptop at home that he used for work purposes" while employed by Siemens, and that Plaintiff copied some of the contents of the flash drives to his personal MacBook that he uses on a daily basis. *See* SOF ¶ 36.

On August 3, 2016, Siemens reminded Plaintiff's counsel that Siemens' property had to be returned to Siemens and that Plaintiff could obtain responsive documents from Siemens via proper requests under Fed. R. Civ. P. 34, so that Siemens could appropriately review the documents for privilege and responsiveness prior to production. *See* SOF ¶ 29, 30. Exhibit 14, August 8, 2016 Letter from Littler, pp. 1-2. Plaintiff's counsel requested that Siemens propose a framework for discovery of files on Plaintiff's flash drives. *See* SOF ¶ 30. When Siemens did so, Plaintiff's counsel thereafter declined to agree to Siemens' proposal or to offer an alternate framework for return of Siemens' property and forensic inspection of Plaintiff's data sources. *See* SOF ¶ 47.

Plaintiff's counsel's actions rise to the level of sanctionable conduct, *see e.g. Burt Hill, Inc. v. Hassan,* 2010 WL 419433, (W.D. Pa. January 29, 2010) (M.J. Bissoon), and cannot be excused by unfamiliarity with how to handle electronic devices and data. *Green v. Blitz U.S.A., Inc.*, 2011 U.S. Dist. LEXIS 20353 (E.D. Tex. Mar. 1, 2011) (criticizing counsel's failure to make a "competent electronic discovery effort"); *Garcia v. Berkshire Life Ins. Co.*, 2007 U.S. Dist. LEXIS 86639 (D. Colo. Nov. 13, 2007) (counsel's "technical incompetence…technical ignorance or mistake is no defense to discovery deficiencies"). Accordingly, in addition to the other requested relief, Siemens seeks the following:

1. An order precluding Plaintiff from using as evidence in this litigation any documents that were not obtained through the discovery process set forth in the Federal Rules of Civil Procedure. *See Burt Hill, Inc. v. Hassan*, No. CIV.A. 09-1285, 2010 WL 419433, at *7 (W.D. Pa. Jan. 29, 2010) (an appropriate sanction would be to prohibit defendants and their lawyers from in any way benefitting from their retention and review of Plaintiff's privileged and confidential information material). *See also Fayemi v. Hambrecht & Quist, Inc.*, 174 F.R.D. 319, 326 (S.D.N.Y.1997) (sanction precluding plaintiff's use of information "would prevent the plaintiff from benefitting from his wrongdoing"); and

2. An award of all fees and cost associated with a forensic examination. *See Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443, 448 (D. Conn. 2010) (apportionment of 80% of forensic expert costs to former employees, where apparent deceit, obstreperousness, and destruction of relevant information on computer hard drives necessitated the retention of the expert).

3. The fees and costs associated with this motion. *Genworth Fin. Wealth Mgmt., Inc. v. McMullan*, 267 F.R.D. 443 (D. Conn. 2010) (awarding sanction of fees and costs where employer had to seek court order to conduct forensic inspection and defendants refused access to computers, and admitted destruction of evidence).

Siemens reserves the right to seek additional sanctions depending on the outcome of the forensic data examination. *See DVComm v. Hotwire Commc'ns,* 2016 U.S. Dist. LEXIS 13661 (E.D Pa. Feb. 3, 2016) (sanctions for destroyed emails based on Fed. R. Civ. P. 37(e) do not preclude further non-monetary sanctions).

III. CONCLUSION

For the foregoing reasons, Defendants' Emergency Motion to Compel the Expedited Return of Defendants' Property, the Preservation of Electronic Data Sources and Production of Data Sources to a Forensic Examiner, and for Sanctions should be granted.

Respectfully submitted,

s/ Allison R. Brown
Robert W. Cameron (PA I.D. No. 69059)
bcameron@littler.com
Allison R. Brown (PA I.D. No. 309669)
arbrown@littler.com
LITTLER MENDELSON, P.C.
EQT Plaza
625 Liberty Avenue, 26th Floor
Pittsburgh, PA 15222
Telephone: 412.201.7600
Facsimile: 412.456.2377

Lauren E. Schwartzreich (NY I.D. No. 4271854)
(pro hac vice pending)
LITTLER MENDELSON, P.C.
900 Third Avenue
New York, NY 10022-3298
Telephone: 212.497.6851

Attorneys for Defendants

Dated: August 19, 2016

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 19th day of August 2016, the foregoing document was filed using the Western District of Pennsylvania's ECF system, through which this document is available for viewing and downloading, causing a notice of electronic filing to be served upon the following counsel of record:

Mark T. Vuono
mvuono@vuonogray.com
Dennis J. Kusturiss
dkursturiss@vuonogray.com
Erica G. Wilson
ewilson@vuonogray.com
VUONO & GRAY, LLC
310 Grant Street, Suite 2310
Pittsburgh, PA 15219

s/ Allison R. Brown